An Enhanced Deterministic Flow Marking Technique to Efficiently Support Detection of Network Spoofing Attacks

Dang Van Tuyen[1], Truong Thu Huong[1], Nguyen Huu Thanh[1], Nguyen Tai Hung[1], Bart Puype[2], Didier Colle[2], Kris Steenhaut[3]

(1) School of Electronics and Telecommunications, Hanoi University of Science and Technology, Hanoi, Vietnam
(2) INTEC, Ghent University, Ghent, Belgium, (3) ETRO, Vrije Universiteit Brussel, Brussels, Belgium
{tuyen.dangvan-set, huong.truong thu, thanh.nguyenhuu, hung.nguyentai}@hust.edu.vn,
{bart.puype, didier.colle}@intec.ugent.be, ksteenha@etro.vub.ac.be

***Abstract*—In order to detect and prevent DoS/DDoS attacks that exploit IP address spoofing, the IP traceback technique has been introduced and developed with variety of methods including packet marking. By means of inserting marking information on the travel path into rarely used fields in the header of IP packets, the destination host can trace back the original-source location of received packets, which is useful for supporting detection of attacks. Many schemes of packet marking IP traceback have been proposed, but still have nevertheless some drawbacks such as low traceback rate, heavy computational overhead due to high-required number of marked packets and marking size. In this paper, we proposed PLA DFM, a novel efficient enhanced solution of Deterministic Flow Marking based on adaptation with real traffic characteristics. The analytic result shows that the proposed solution provides a far higher successful mark rate, lower computational overhead compared to the original scheme and other marking techniques with unnoticeable increased traffic size.**

Keywords—DoS/DDoS, IP Spoofing, IP traceback, Packet Marking, Deterministic Packet Marking, Derterministics Flow Marking.

I. INTRODUCTION

Nowadays, Denial of Service (DoS) and Distributed Denial of Service (DDoS) remain the largest challenges of network security. In DoS/DDoS attack, the attackers may generate and send a huge number of attack packets to the victim in a short period of time. Due to the stateless and anonymous nature of the Internet, attackers can easily spoof the source IP address. It is extremely difficult for the attack detection and prevention solutions to identify the real original source of the attack. To address this problem, the IP traceback technique has been introduced as a way to support schemes of attack detection [2][3][4][5][6][8].

The traceback technique enables victims to reconstruct the travel path of a specific packet or to know the address of the location in which the packet originated regardless of whether the IP source address contained in the packet is spoofed or not. Traceback is neither the solution of attack detection nor attack prevention, but this technique can support these solutions to know the real source of suspicious packets during or after attack without using the source IP address field in the IP header. Traceback techniques can be classified into 5 main categories: link testing, messages, logging, packet marking and hybrid schemes. In link testing schemes, the attack sources are traced manually from victims to upstream links for finding the links, which carry the attacked traffic. The message schemes use ICMP messages to reconstruct the travel path of the packets. Logging schemes query logged databases maintained at every router on the travel path and apply some data mining algorithms to determine the origin of the packet. Packet marking schemes try to insert into the IP header some router information, which can be used for identifying the original source location of packets. This paper focuses on the fourth group, packet marking. In fact, there are several packet-marking–based traceback proposals, but the problem of relatively low successful marking with a high number of processed packets still remains.

In this paper, we focus on packet-marking-traceback technique and propose the PLA DFM (Packet Length Adaptive Deterministic Flow Marking) scheme, an enhanced solution of the packet marking traceback technique DFM Based on the result of analyzing the real network traffic from the CAIDA 2013 dataset [1], we evaluate the performance of PLA DFM. The result shows that PLA DFM has a much higher rate of successful marking compared to the original DFM. The marked packet rate and the marked size rate are lower than DFM with a slightly increased size.

The rest of the paper is structured as follows: Section II provides an overview of the related work and background on marking traceback techniques. Section III describes some characteristics of real network traffics, limitation of the DFM technique and the main principle of our solution so-called PLA DFM, which is the modified enhanced version of DFM. Section IV analyzes the performance of PLA DFM and makes a comparison to the original one. Section V presents the conclusion of the paper and some future work.

II. RELATED WORK AND BACKGROUND ON PACKET MARKING IP TRACEBACK

In the packet marking traceback technique, marking information of some or all routers in the travel path is sent to the destination. Marking information is often the addresses of

routers. The destination uses this information for tracing back to the location of the original source of the packets without using the IP source address field in the IP header. A marking process inserts the marking information into rarely-used fields in the IP header before forwarding packets to the destination. There are two main techniques of packet marking: PPM (Probabilistic Packet Marking) and DPM (Deterministic Packet Marking).

A. PPM and DPM

Introduced by Savage et al.[2], in PPM all routers on the travel path of a packet are involved in the marking process. Packets passed through a router will be marked based on a fixed probability p=0.04. Marking information is the edge between the current router and the previous one. The edge-id is produced by the "XOR" of IP addresses of these two nodes and divided into small segments. Each segment is selected randomly to be stored inside 16 bits of Identification field in the header of a marked packet as a sample of the travel path. When the destination receives enough samples, the path can be reconstructed. The main advantages of the PPM scheme are: simple, easy to implement, no increment of packet size, and relatively low marking computational overhead at routers. However, the noticeable drawbacks are the high overhead requirement for path reconstruction at the destination, low successful-traceback rate, and the problem of overwriting the information in marked packets that leads to a high false rate [11].

In order to overcome the disadvantages and improve the efficiency of PPM, some other proposals have been introduced. J. Liu, et al. used dynamic probability based on TTL decrement for selecting marking packets in Dynamic PPM scheme (DPPM) [3]. V. Paruchuri, et al. proposed the Authenticated AS traceback [4], in which the AS (Autonomous System) number is used instead of the IP addreses. The scheme also changes the probability to fixed value of 1/6. Similarly, the Efficient AS DoS Traceback (EAST) scheme [5] introduced by Mohammed Alenezi et al. uses AS number as marking information with the dynamic probability p=1/(a-2) where a is the AS distance from the source to the destination. EAST scheme also uses, 8 bits of TOS fields in the IP header for marking containers and therefore the entire marking information of each AS can be put in only one packet. However, these schemes do not decrease much the computational overhead at the destination.

Introduced by Belenky et al.[6][7], DPM marks IP packets of ingress traffics only at edge routers of ISP networks. The marking information is the IP address of the ingress port on edge routers. 16 bits of the Identification field are used for storing marking information and the Reserved Flag bit is used for indicating if the packet is marked or not (Marked Flag). 32 bits of marking information are segmented into small parts, which can be embedded in the header of an IP packet. During DPM marking, each segment is selected with probability p=1/K where K is the number of packets required for marking. DPM can traceback under DoS attacks better than PPM and can be used in on-the-fly systems thanks to the lower computational requirement at the destination. Besides, the scheme does not increase packet size and can prevent attackers from spoofing marking. However, the false positive rate is still relatively high especially under DDoS attacks.

For enhancement, the extended DPM [8] proposed by V.K. Soundar Rajam et al. and the flexible DPM [11] introduced by Yang Xiang et al. use 8 bits more from the TOS field to expand the marking container up to 25 bits. This modification decreases the required number of packets for successfully tracing back but may result in collision because these bits have been used for Differentiated Services Code Point (in RFC 2474) [9] and Explicit Congestion Notification (in RFC 3168) [10]. Although these enhanced solutions improve the efficiency, DPM schemes still retain some chronic drawbacks including: high computational requirement and low accurate tracebacked location.

B. Deterministic Flow Marking (DFM) Technique

Proposed by Vahid Aghaei-Foroushani et al.[12], DFM is an improved scheme of DPM. Like DPM, the marking process of DFM is carried out at edge routers for ingress traffic. However, DFM does not mark all incoming packets but only K first packets for each incoming flow. A TCP/UDP flow is defined by 5-tuple parameters including source and destination IP addresses, L4 protocol type, source and destination ports. For determining an ICMP flow, 6-tuple parameters are used: source and destination IP addresses, L4 protocol type (ICMP), ICMP Code, ICMP Type and ICMP ID. Besides, there are two constraint parameters:

- Inactive Timeout: the interval between two consecutive unidirectional packets in a flow must be smaller than Inactive Timeout, otherwise those two packets belong to two flows.
- Active Timeout: the existing time of a flow shall not exceed Active Timeout

If one of these two criteria is violated, a flow is discarded and a new one is created for the next packet. In DFM, the marking information is expanded up to 60 bits including:

(i) 32 bits of IP address of an egress port on the edge router, where a flow is forwarded to the next hop,

(ii) 12 bits of NIID, the unique value indicates the MAC address or VLAN ID of ingress port, where the flow enters to the Internet and

(iii) 16 bits of NodeID, the value to identify the unique host sending the flow to the edge router.

The number of packets needed for marking in each flow depends on the usage of the fields in the IP header for containing marking information. DFM does not specify the fields in the IP header that can be used for marking. Except for the 16 bits of Identification and 1 bit of Reserved Flag, the scheme can use other rarely-used fields, including 8 bits of TOS and 13 bits of Fragment Offset. TABLE I. shows the required numbef of packets K for a successfully-marked flow depending on the usage of the fields in IP header for marking.

TABLE I. THE USAGE OF FIELDS AND REQUIRED PACKET NUMBER IN EACH FLOW FOR MARKING IN DFM

Used fields	Size of marking space (bits)	*K*
Identification, Reserved Flag, TOS and Fragment Offset	37	2
Identification, Reserved Flag and TOS	25	3
Identification, Reserved Flag and Fragment Offset	30	3
Identification and Reserved Flag	17	5

Marking just only K first packets in each flow, in comparison to DPM, the number of marked packets decreases by as much as nearly 90% [12]. Therefore, the computational

overhead of marking at edge routers is also reduced. Furthermore, by adding more details in marking information, DFM scheme provides the ability to trace back closer to the original source. Besides, in order to ensure that compromised routers in the network path have not changed the marking information, the DFM scheme introduces the option of authentication. Thanks to receiving public keys of edge routers, the destination could verify the marking information and eliminate possibility of modification by malfunctioning routers.

III. OUR PROPOSED PACKET LENGTH ADAPTIVE DFM

Due to the outperforming characteristics of the DFM technique, it inspired us to study and develop an enhanced version of the DFM scheme. In order to understand better the pending problem of DFM that we try to solve, we at first analyze the DFM's marking performance that essentially depends on the Internet traffic characteristics.

A. Analysis of the Internet traffic characteristics and the DFM's performance

To improve the efficiency in marking IP traceback, it is necessary to reduce the number of marked packets. Although the number and total size of marked packets decrease much and a higher traceback rate can be gained in comparison to DPM, DFM needs fixed *K* first packets in each flow for holding marking information. A flow, which has less than *K* packets, will not be marked successfully and therefore the destination will not be able to trace the origin of those packets.

To study the rate of successful marking in DFM, we analyzed and got statistics of packet distribution and length of the first packet in each flow from 5 million flows in CAIDA 2013 traffic dataset [1]. We have employed the Scapy tool [16] to get sequenced packets in the traffic dataset and assign them into flows. The value of INACTIVE TIMEOUT and ACTIVE TIMEOUT were set to 15 seconds and 30 minutes respectively, these values were chosen based on the default values of some other prevalent protocols such as NetFlow [13]. For each flow, we recorded the number of packets and the first packet length then stored the information into a database. The analysis result presented in Fig. 1 is extracted by querying the database. As seen in Fig. 1, flows that have only one packet account for a major portion (over 40%). With this distribution, even in the case of K=2, the rate of successful marking is quite low (under 60%).

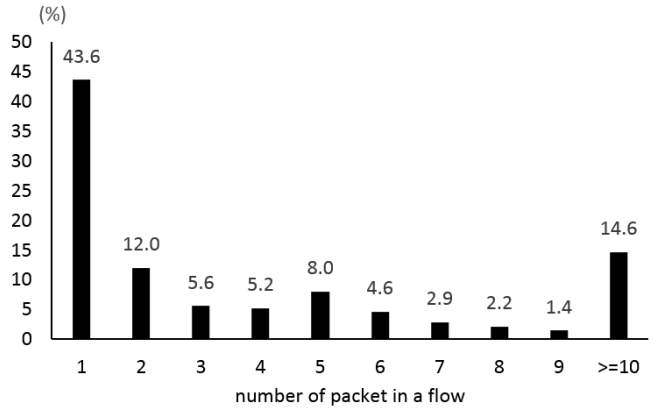

Fig. 1. Distribution of number of packets in a flow

In DFM, the higher the number of packets needed for marking, the lower success rates of marking. In order to increase the capability of successful marking, marking information should be carried out in as few packets as possible. Instead of putting marking information to headers of *K* packets, more fields in the IP header are used to afford 60-bit DFM marking information. By means of involving more fields in the IP header for marking, the fewer packets in a flow are needed, consequently producing a higher traceback rate.

B. Packet Length Adaptive DFM

The main idea of our proposed enhanced DFM version - PLA DFM has two main purposes:

(1) PLA DFM tries to push all marking information into the first packet where possible in order to reduce the required number of marked packets, consequently increasing the marking rate.

(2) A length threshold **MT** is set to avoid packet fragmentation

It can be seen that with the IP header fields used in DFM, 60 bits marking information could not be inserted entirely into the header of only 1 packet. Hence, in our PLA DFM, the Options field is used with the length of 2 datagram units, equivalent to 8 bytes. PLA DFM also introduces another problem: the required expansion of the IP header may increase the packet size beyond the network path MTU, and lead to fragmentation. However, as seen in Fig. 2, lengths of the first packet in most flows are relatively small. Nearly 90% of flows have the first packet size varying under 200 bytes, whilst the total packet range can be up to 1500 bytes. Therefore, if a length threshold is defined and this marking method is applied just for flows that have the first packet length smaller than the threshold, the rate of successful marking will be improved.

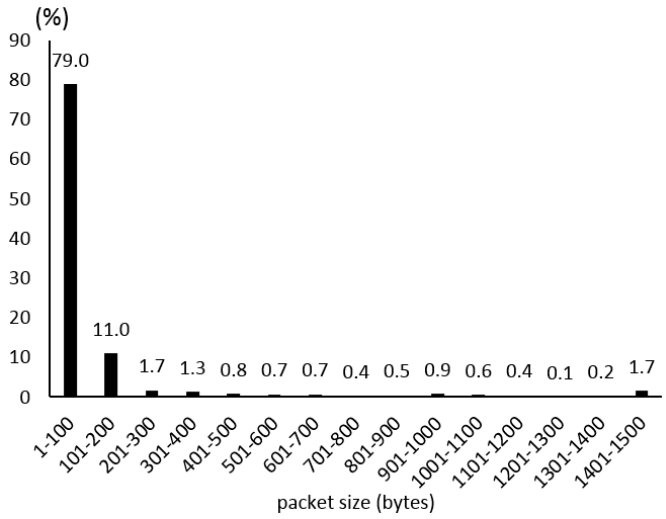

Fig. 2. Distribution of length of the first packet

Like DFM, PLA DFM marking process is handled just only at edge routers of ISP networks and applied for the ingress traffic. The marking information for each arrival ingress flow comprises 32 bits of egress IP address, 12 bits of NIID and 16 bits of NodeID. In order to distinguish a marked packet from unmarked ones, 1 Marked Flag bit is indicated. PLA DFM uses Reserved Flag for this indication. If the Reserved Flag bit is set to 1, the packet is marked and vice versa, the packet is a normal one if Reserved Flag is zero. As discussed above, we define a threshold of packet length called **Mark Threshold** (**MT**). In PLA DFM, marking information of each flow is conveyed in two manners:

Manner 1: If the first packet length is smaller than or equal to **MT**, PLA DFM exploits 16 bits of the ID field and 48 bits of

the Options field for placing marking information as seen in Fig. 3.

Manner 2: If the first packet length is greater than MT, marking information is put into the rarely used fields in the IP header of *K* first packets in the same way the original DFM scheme does (i.e. Identification, Reserved Flag, TOS and Fragment Offset field).

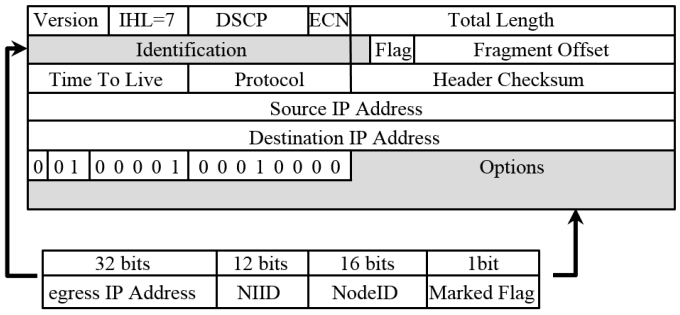

Fig. 3. Header structure of the first packet marked by PLA DFM Manner 1

However, in order to avoid the conflict, which may be caused with Differentiated Services Code Point (in RFC 2474) [8] and Explicit Congestion Notification (in RFC 3168) [9], PLA DFM does not employ the TOS field as the marking container. Consequently, only the two later circumstances in Table I are developed in our PLA DFM:

(1) Insert marking information in the header of 3 first packets (*K*=3). The fields of Identification, Reserved Flag and Fragment Offset are used for marking and the total container size is T=30 bits in each marked packet. Due to segmentation, except for M=20 bits marking information segment, each marked packet needs $S=\log_2(3)=2$bits for segment order.

(2) Insert marking information in the header of 5 first packets (*K*=5). The fields of Identification and Reserved Flag are deployed. In this case, the values are T=17, S=3 and M=12.

As the marking information is divided into segments and sent in different IP packets, if there are concurrently many sources spoofing the same flow properties and sending packets to the same destination, the victim may not be able to distinguish the origin of received marking segments and hence may be confused trying to trace separately these sources. To prevent this problem, the option of using a marking checksum is introduced in PLA DFM. A checksum value is calculated from marking information for each flow and sent along with a segment in each marked packet. By comparing received checksum values, the destination host can differentiate the origins of marking segments and reconstruct accurately the marking information even if it receives packets from many sources that spoof the same flow properties.

The option of using marking checksum results in requirement of more space in marked packets. For the scheme of *K*=3 with a total of 30 dedicated bits, 1 bit is used for Marked Flag, *M*=20 bits for marking information segment, *S*=2 bits for segment order, there are up to *C*=7 bits in each packet used for holding the marking checksum value. In this scheme, *K*=3 packets are enough for successfully marking, both with or without marking checksum option. Whilst in the case of *K*=5 with a total of 17 dedicated bits, 1 bit is used for Marked Flag, *M*=12 bits for marking segment, *S*=3 bits for segment order, there is not enough space for checksum value. To use this option, there must be *K*=7 packets for marking successfully a flow and these parameters are *M*=12, *S*=3 and *C*=4 bits for checksum value.

An important factor in PLA DFM is to set the marking threshold MT value. Choosing a small MT decreases the number of flows marked by expanding the packet header, and results in having a lower rate of successful marking, but eliminates the risk of packet fragmentation. The MT value is selected based on the minimum MTU of network links in the network path. Because 8 bytes are added onto the header of each packet marked by this method, the MT value may be calculated by subtracting 8 bytes from the minimum MTU. TABLE II. lists MTU link values of some common physical networks [14][15] and the corresponding MTs.

TABLE II. SOME COMMON MTUS AND CORRESPONDING MTS [14][15]

Physical net work	MTU	MT
Point To Point (RFC1661)	296	288
ARCNET	508	500
X. 25	576	568
IEEE 802.3	1492	1484
Ethernet	1500	1492

The marking algorithm with the option of using marking checksum at edge routers is presented in TABLE III.

TABLE III. THE ALGORITHM OF PLA DFM WITH THE OPTION OF USING MARKING CHECKSUM

```
1.FOR EACH arrival_packet
2.  IF arrival_packet belongs to an existed active current_flow THEN
3.      IF current_flow.NeededPackets >0 THEN
4.          CALL current_flow.DFM_Marking with arrival_packet
5.  ELSE
6.      INIT  new_active_flow
7.      OBTAIN Marking_Information
8.      IF arrival_packet.Total_length <= MT THEN
9.          SET arrival_packet.Ihl_field to arrival_packet.Ihl_field + 2
10.         PUT Marking_Information into arrival_packet.Id_field
                and arrival_packet.Options_field
11.         SET arrival_packet.Reserved_Flag to 1
12.         SET new_active_flow.NeededPackets to 0
13.     ELSE
14.         CALCULATE DFM_Check_Sum with
                Marking_Information
15.         PUT Marking_Information and DFM_Check_Sum
                into arrival_packet Marking_Segments_Array
16.         SET new_active_flow.NeededPackets to K
17.         CALL current_flow.DFM_Marking with arrival_packet
18. RECALCULATE arrival_packet.IP_Header_Checksum
19. FORWARD arrival_packet
20. FOR EACH active_flow
21.     IF active_flow.Is_TimeOut THEN
22.         DISPOSE active_flow

23.flow.DFM_Marking (packet)
24.     PUT flow. Marking_Segments_Array[K-flow.NeededPackets]
            into packet.Id_field and packet.FragmentOffset_field*
25.     SET packet. Reserved_Flag to 1
26.     DECREAMENT flow.NeededPackets
```

* applied for K=3

IV. PERFORMANCE EVALUATION

In order to evaluate the efficiency of the proposed solution and compare to the original DFM, we analyze the real network traffic from CAIDA 2013 dataset, then evaluate performance statistically for both DFM and PLA DFM solutions with 3 schemes: *K*=3, *K*=5 and *K*=7.

In the schemes of K=3 and K=7, PLA DFM adopts the option of either using marking checksum or not. For the K=5 circumstance, the marking checksum option is not supported due to lack of space for containing this value. Concerning the marking threshold, we start at MT=288 with the assumption that the Point To Point (in RFC 1661) [15] appears commonly in most of network paths because this protocol is used over many types of physical networks and supports most of transmission standards such as Ethernet, ATM, SONET/SDH, etc. Moreover, the MTU value set by the protocol is quite lower than the ones of other data link protocols. To study the effectiveness of choosing MT thresholds, we also analyze and get statistical parameters for other MTs and compared to the first case.

Practically, we developed a Scapy-based python tool, which can extract, read characteristics of every packet in the dataset and assign them into flows. The Sqlite database tool [17] is employed to manage all extracted flows. For accuracy, only completed flows are taken into account (i.e. flows in which one of the two TIMEOUT conditions described in II.B is met). The completed flows are tracked continuously in time in the dataset. After each 100.000 completed flows, we get the statistics and calculate some major metrics for each scheme. It shows that the starting point of traffic capture affects the performance much. As seen in Fig. 4 Fig. 5 Fig. 6, performance at the beginning is fluctuated strongly since a lot of ongoing flows are captured in the middle of the flows at the starting point. When the number of flows is big enough, the impact of the starting point fades out and the performance gets stable. The calculated metrics used for the performance comparison include:

1. Successful mark rate (SMR): The rate between number of flows that have enough packets to carry entirely marking information and total flow number in the traffic.
2. Marked packet rate (MPR): The number of marked packets out of total packet number in the traffic.
3. Marked size rate (MSR): The total size of marked packets including expansion amount (if applicable) out of the size of entire traffic.

Fig. 4 Fig. 5 and Fig. 6 show the successful mark rate of PLA DFM scheme with MT=288 outperforming DFM in all 3 cases. As shown in Fig. 4, the successful mark rate of PLA DFM maintains stable over 95% (K=3), 94% (K=5) and 93% (K=7) while marking rate of DFM is just under 45%(K=3), 35% (K=5) and 25% (K=7).

Regarding the marked packet rate, PLA DFM marks fewer packets in each flow and consequently the rate is lower than DFM as shown in Fig. 5 The mark packet rate of DFM in case of K=3, K=5 and K=7 are about 8%, 11% and 13% respectively while the MPR of PLA DFM is approximately 5%.

Similarly, the total size of marked packets in PLA DFM is considerably smaller than the marked size in DFM. As seen in Fig. 6, with the same K, the marked size rate of PLA DFM is just half of the DFM marked size rate. The comparison among PLA DFM schemes with various K and MT values in TABLE IV. shows that the successful mark rate, marked packet rate and marked size rate are changed unnoticeably. The reason is that most of the first packets in flows have a size smaller than 200 bytes. Therefore, incrementing of MT does not affect much the number of flows marked by using the Options field in the IP header. With this result, the MT value around 288 should be used to tradeoff between a high successful mark rate and the risk of packet fragmentation.

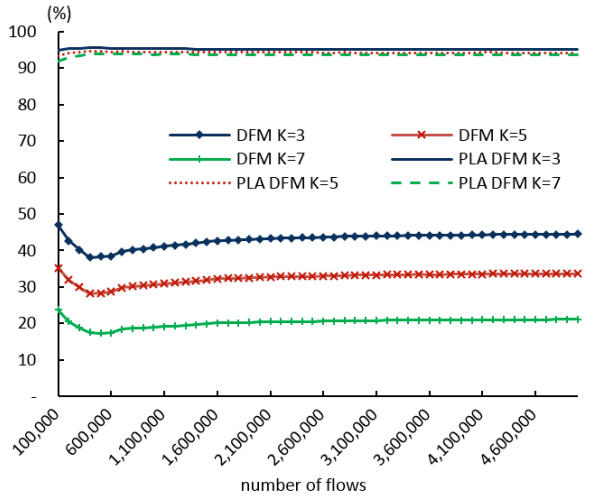

Fig. 4. SMR of DFM schemes and PLA DFM schemes with MT=288

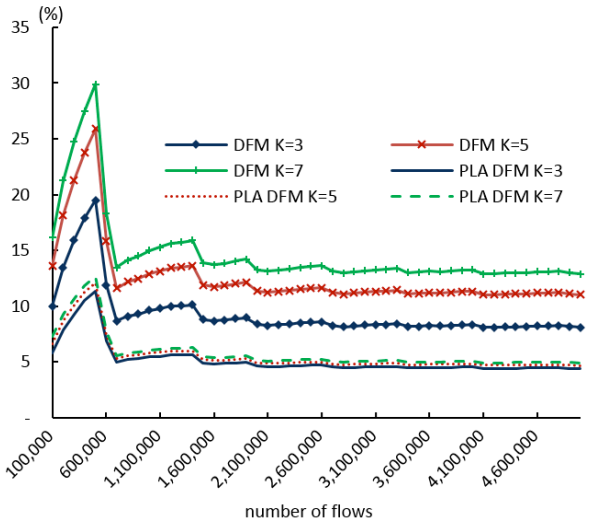

Fig. 5. MPR of DFM schemes and PLA DFM schemes with MT=288

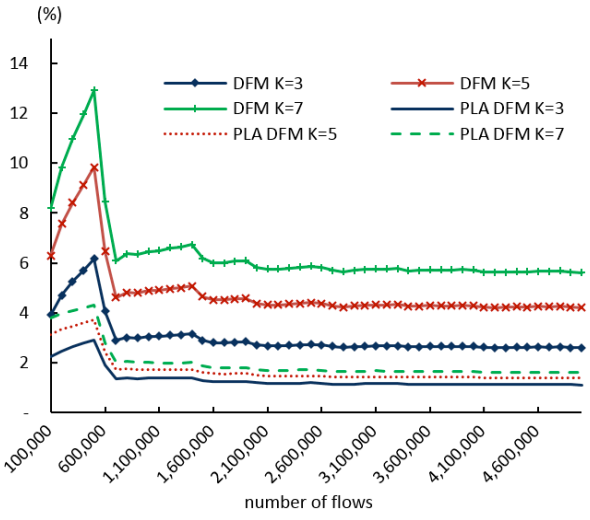

Fig. 6. MSR of DFM schemes and PLA DFM schemes with MT=288

TABLE IV. COMPARISON OF DIFFERENT PLA DFM SCHEMES WITH VARIOUS *K* AND MT

MT	K	SMR	MPR	MSR
288	3	95.11	4.40	1.11
	5	94.26	4.68	1.39
	7	93.66	4.91	1.61
500	3	96.95	4.36	1.09
	5	96,65	4.58	1.35
	7	96.15	4.78	1.56
568	3	97.18	4.26	1.07
	5	96.92	4.55	1.34
	7	96.46	4.74	1.55

Survey on 5 million flows in the traffic of the CAIDA 2013 dataset

In PLA DFM, with the flows marked by using expansion of Options field, the additional packet length leads to an increase of total traffic size in the network. As seen in TABLE V. the increased size is not considerable compared to the total traffic size. The increased size rate does not depend on *K* and maintains stable under 0.05% with various MT values.

TABLE V. THE RATE OF INCREASED SIZE IN PLA DFM

MT	Total original size (bytes)	Increased size (bytes)	Rate (%)
288	85,209,121,130	36,390,376	0.043
500	85,209,121,130	37,503,744	0.044
568	85,209,121,130	37,668,640	0.044

V. CONCLUSION AND FUTURE WORK

In this paper, we propose an enhanced solution of packet marking IP traceback - PLA DFM and compare the solution with the original DFM scheme with 4 major metrics: the successful mark rate, marked packet rate, marked size rate and the percentage of increased size.

According to the research result, PLA DFM makes use of the characteristics of the actual traffic that the length of the first packet in each flow is often smaller than that of the others; and the flows which have number of packets smaller than needed one for successfully marking by DFM accounts for a major portion and improves performance. Using a flexible mechanism in marking decided by the length of the first packet, the successful mark rate of PLA DFM is respectably higher than the original scheme with the unnoticeable increase of the packet size. Moreover the amount and total size of marked packets are much decreased in comparison with the original DFM. These are useful for implementation using independent equipment attached outside edge routers.

For future work, the research will focus on the capacity of marking and traceback in the condition of denial of service attack, application and implementation of the scheme in detecting and preventing attacks on the fly. Measurement of some system parameters such as computational overhead, response time etc. also needs to be carried out.

ACKNOWLEDGMENT

This work is supported by the PhD Program in HUST, Vietnam as well as the Lotus Project within the Framework of the Erasmus Mundus Action 2 for Mr.Tuyen's research exchange to Vrije Universiteit Brussel and Universiteit Gent, Belgium.

REFERENCES

[1] The CAIDA UCSD Anonymized Internet Traces 2013, http://www.caida.org/data/passive/passive_2013_dataset.xml

[2] S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Network support for IP traceback," IEEE/ACM Transactions on Networking, Vol. 9, no. 3, pp. 226-237, June 2001.

[3] J. Liu, et al., "Dynamic probabilistic packet marking for efficient IP traceback," Computer Networks, vol. 51, pp. 866-882, 2007.

[4] V. Paruchuri, et al., "Authenticated autonomous system traceback," in 18th International Conference on Advanced Information Networking and Application (AINA'04), 2004, pp. 406-413 Vol. 1.

[5] Mohammed Alenezi et al., "Efficient AS DoS Traceback," in Proceeding of 2013 International Conference on Computer Applications Technology (ICCAT), January 2013, Sousse, Tunisia.

[6] A. Belenky et al., "IP traceback with deterministic packet marking," IEEE Communications Letters, vol. 7, no. 4, pp. 162-164, April 2003.

[7] A. Belenky et al., "Tracing Multiple Attackers with Deterministic Packet Marking (DPM)," in Proceeding of 2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM '03), Victoria, B.C., Canada, August 28-30, 2003, pp. 49-52.

[8] V.K. Soundar Rajam et al., "A novel traceback algorithm for DDoS attack with marking scheme for online system," in Proceeding of 2012 International Conference on Recent Trends In Information Technology (ICRTIT), April 2012, Chennai, Tamil Nadu, India.

[9] K. Nichols et al., "Definition of the Differentiated Services Field (DS Field)in the IPv4 and IPv6 Headers", December 1998, available online at http://tools.ietf.org/html/rfc2474.

[10] K. Ramakrishnan et al., "The Addition of Explicit Congestion Notification (ECN) to IP", September 2001, available online at http://tools.ietf.org/html/rfc3168.

[11] Xiang et al., "Flexible deterministic packet marking - an IP traceback system to find the real source of attacks", IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 4, pp. 567-580.

[12] Vahid Aghaei-Foroushani et al., "On Evaluating IP Traceback Schemes: A Practical Perspective," spw, pp.127-134, 2013 IEEE Security and Privacy Workshops, 2013.

[13] Cisco Systems, Inc, "Cisco IOS NetFlow Command Reference", July 2011, p. 56, availabe online at http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/command/nf-cr-book.pdf.

[14] Martin P.Clack, "Data Networks, IP and the Internet: Protocol, Design and Operation", John Wiley & Sons Inc, 2003, ISBN: 0-470-84856-1, p. 181.

[15] Mario Marques da Silva, "Multimedia Communications and Networking", CRC Press, 2012, ISBN: 978-1-4398-7484-4, p.364.

[16] http://www.secdev.org/projects/scapy/

[17] http://www.sqlite.org/